На правах рукописи

Разинков Евгений Викторович

# МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ СТЕГАНОГРАФИЧЕСКИХ ОБЪЕКТОВ И МЕТОДЫ ВЫЧИСЛЕНИЯ ОПТИМАЛЬНЫХ ПАРАМЕТРОВ СТЕГОСИСТЕМ

Специальность 05.13.18 – Математическое моделирование,
численные методы и комплексы программ

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата физико-математических наук

Казань – 2012

Работа выполнена в федеральном государственном автономном образовательном учреждении высшего профессионального образования «Казанский (Приволжский) федеральный университет» на кафедре системного анализа и информационных технологий.

**Научный руководитель** доктор технических наук, профессор
**Латыпов Рустам Хафизович**

**Официальные оппоненты:** доктор физико-математических наук, профессор
**Соловьев Валерий Дмитриевич**
(Казанский (Приволжский) федеральный университет, г. Казань)

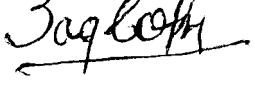
доктор технических наук, профессор
**Файзуллин Рашит Тагирович**
(Омский государственный технический университет, г. Омск)

**Ведущая организация**: Санкт-Петербургский институт информатики и автоматизации РАН, г. Санкт-Петербург.

Защита состоится 13 декабря 2012 г. в 15:30 на заседании диссертационного совета Д 212.081.21 в Казанском (Приволжском) федеральном университете по адресу: 420008, г. Казань, ул. Кремлевская, 18, корп. 2, ауд. 218.

С диссертацией можно ознакомиться в Научной библиотеке им. Н.И. Лобачевского Казанского (Приволжского) федерального университета.

Автореферат разослан «___» ноября 2012 г.

Ученый секретарь
диссертационного совета Д 212.081.21
д.ф.-м.н., профессор  Задворнов О.А.

# ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

## Введение

Диссертационная работа посвящена разработке теоретико-информационного подхода к построению математических моделей стеганографических объектов, построению математической модели цифрового изображения в формате JPEG, разработке эффективных алгоритмов целочисленной минимизации сепарабельной функции, исследованию свойств стеганографических систем.

## Актуальность темы

Цифровая стеганография – наука о скрытой передаче информации, которая часто осуществляется за счет встраивания передаваемого сообщения в некий не вызывающий подозрения цифровой объект путем незначительной его модификации. Результат встраивания передается по каналу связи получателю, который извлекает встроенное сообщение. Это эффективное средство защиты информации, становящееся особенно актуальным в случае, когда применение криптографических методов невозможно или ограничено.

Все применяемые на практике стегосистемы и стегоаналитические атаки явно или неявно опираются на модели стеганографических объектов – контейнеров, в которые встраивается информация, и стего, получаемых в результате встраивания. Чем более точной моделью стеганографических контейнеров располагает стеганограф, тем более стойкую к стегоаналитическим атакам стегосистему он способен построить. И наоборот, если стегоаналитик располагает более точной моделью контейнеров, нежели стеганограф, он часто будет иметь возможность построить эффективную стегоаналитическую атаку. Таким образом, построение более точных моделей стеганографических объектов – актуальная задача, стоящая перед исследователями в области цифровой стеганографии и стегоанализа.

Отметим отсутствие моделей, которые бы опирались на теоретико-информационный подход к стеганографической стойкости, но в то же время

учитывали свойства форматов используемых на практике стеганографических объектов и могли непосредственно использоваться для исследования и совершенствования практических стеганографических систем и стегоаналитических атак. Наличие каждого из этих свойств у математической модели обеспечивает связь между теоретическими основами цифровой стеганографии и практическим применением стеганографических средств защиты информации, обеспечивая тем самым возможность применения существующих теоретических результатов для оценки стойкости современных стегосистем.

JPEG (Joint Photographic Experts Group) – один из самых распространенных форматов цифровых изображений в сети Интернет, что делает его наиболее привлекательным для встраивания информации стеганографическими методами, а потому задача математического моделирования цифровых изображений в формате JPEG особенно актуальна.

**Цель и задачи диссертационной работы**

Целью диссертационной работы является исследование влияния различных факторов на стойкость стеганографических систем и разработка методов вычисления оптимальных параметров встраивания информации. Для достижения этих целей были поставлены и решены следующие задачи:

1. Исследовать существующие подходы к математическому моделированию стеганографических объектов, способы оценки и повышения стойкости стегосистем;
2. Предложить теоретико-информационный подход к построению математических моделей стеганографических объектов;
3. Построить математическую модель цифрового изображения в формате JPEG, позволяющую исследовать влияние параметров стегосистемы и других факторов на стеганографическую стойкость;
4. Предложить метод повышения стойкости стегосистем в рамках предложенной модели;

5. Разработать эффективные вычислительные алгоритмы решения задач минимизации, возникающих при исследовании математических моделей стеганографических объектов;
6. Реализовать разработанные модели, методы и алгоритмы в виде комплекса программ, позволяющего исследовать проблему оценки и повышения стойкости стегосистем с помощью численных экспериментов;
7. Исследовать влияние параметров скрывающего преобразования и других факторов на стойкость стеганографической системы путем проведения вычислительного эксперимента.

**Методы исследования**

В диссертационной работе применялись методы теории вероятностей, нелинейного программирования, математического моделирования.

**Научная новизна**

В диссертационной работе получены следующие новые научные результаты:

1. Предложен теоретико-информационный подход к построению математических моделей стеганографических объектов, основанный на вычислении относительной энтропии;
2. Разработана математическая модель цифрового изображения в формате JPEG, позволяющая исследовать влияние количества встраиваемой информации, стратегии встраивания, свойств изображений-контейнеров, выбранного вектора характеристик на стеганографическую стойкость;
3. Предложен метод нахождения оптимальной стратегии встраивания информации для заданного вектора характеристик;
4. Разработан эффективный вычислительный алгоритм решения возникающей при нахождении оптимальной стратегии стеганографа задачи минимизации сепарабельной функции;

5. Разработан комплекс программ, реализующий модель цифрового изображения в формате JPEG, алгоритмы минимизации функции относительной энтропии и метод нахождения оптимальной стратегии встраивания информации;
6. Исследовано влияние количества встраиваемой информации, стратегии встраивания, выбранного вектора характеристик, фактора качества изображений, используемых в качестве контейнеров, на стойкость стеганографической системы путем проведения вычислительного эксперимента.

**Практическая значимость работы**

Разработанный подход к математическому моделированию стеганографических объектов позволяет строить модели стеганографических объектов различных форматов, обеспечивающие возможность:

- исследовать стойкость стеганографических систем к наилучшей возможной стегоаналитической атаке, использующей заданный вектор характеристик;
- вычислять оптимальные и субоптимальные стратегии встраивания информации;
- исследовать влияние стратегии встраивания информации, параметров стегосистемы, векторов характеристик, свойств используемых контейнеров на стойкость стегосистемы.

Предложенная математическая модель цифрового изображения в формате JPEG позволяет оценить влияние различных факторов на стойкость встраивания информации алгоритмом nsF5 к наилучшей возможной стегоаналитической атаке, использующей характеристики изображения, составляющие основу наборов характеристик, применение которых в универсальном стегоанализе показано экспериментально. Факторы, влияние которых на стойкость стегосистемы может быть исследовано с помощью

математической модели изображения и реализующего эту модель комплекса программ:

- количество встраиваемой информации;
- стратегия встраивания, заключающаяся в распределении встраиваемой информации между группами DCT-коэффициентов;
- используемый вектор характеристик, пороговые значения используемых характеристик;
- фактор качества и другие свойства изображений-контейнеров.

Возможность проведения анализа влияния этих факторов на стеганографическую стойкость позволяет находить оптимальные и субоптимальные стратегии встраивания информации, совершенствовать стегосистемы и стегоаналитические атаки.

**Апробация работы**

Основные результаты диссертационной работы докладывались на следующих научных конференциях и семинарах:

1. Научная школа-семинар с международным участием «Компьютерная безопасность и криптография» SIBECRYPT'10, ТюмГУ, г. Тюмень.
2. Научная школа-семинар с международным участием «Компьютерная безопасность и криптография» SIBECRYPT'09, ОмГУ, г. Омск.
3. Семинар на кафедре системного анализа и информационных технологий ИВМиИТ, КФУ, г. Казань.
4. Семинар в Санкт-Петербургском институте информатики и автоматизации РАН (СПИИРАН), г. Санкт-Петербург.
5. IEEE 6th Conference on Cybernetic Systems, 2007, UCD, Dublin.
6. Общероссийская конференция «Математика и безопасность информационных технологий» MaBIT'06, МГУ, Москва.

На защиту выносятся следующие результаты:

1. Теоретико-информационный подход к построению математических моделей стеганографических объектов, обеспечивающий возможность оценки стойкости стегосистемы к наилучшей возможной атаке, использующей заданный вектор характеристик.
2. Математическая модель цифрового изображения в формате JPEG, позволяющая исследовать влияние количества встраиваемой информации, стратегии встраивания, свойств изображений-контейнеров и других факторов на стойкость стегосистемы к наилучшей возможной атаке, использующей заданный вектор характеристик;
3. Метод нахождения оптимальной стратегии встраивания информации, обеспечивающей повышение стойкости стегосистемы.
4. Эффективный вычислительный алгоритм минимизации сепарабельной функции.
5. Комплекс программ, реализующий модель цифрового изображения в формате JPEG, метод нахождения оптимальной стратегии встраивания, алгоритмы минимизации функции относительной энтропии.
6. Результаты численного исследования влияния размера скрываемого сообщения, стратегии встраивания, выбранного вектора характеристик, свойств изображений-контейнеров на стойкость стеганографической системы.

**Структура и объем диссертации**

Диссертационная работа состоит из введения, четырех глав, заключения и списка использованных источников, содержащего 67 наименований. Объем диссертационной работы составляет 109 страниц, работа содержит 16 рисунков и 7 таблиц.

## СОДЕРЖАНИЕ РАБОТЫ

Во **введении** обоснована актуальность выбранной темы, ее научная и практическая значимость.

В **первой главе** приведен обзор существующих подходов к исследованию свойств стеганографических систем и моделированию стеганографических объектов. Выявлено отсутствие моделей, которые бы опирались на теоретико-информационный подход к стеганографической стойкости, но в то же время учитывали свойства форматов цифровых объектов, используемых на практике, и могли непосредственно применяться для исследования и совершенствования существующих стеганографических систем.

В целях обоснования расставленных в работе приоритетов при построении математической модели рассмотрены существующие подходы к понятию стеганографической стойкости, существующие способы ее повышения, проведен анализ существующих методов встраивания информации и современных методов стегоанализа.

**Вторая глава** посвящена математическому моделированию стеганографических объектов, построению математической модели цифрового изображения в формате JPEG.

*Теоретико-информационный подход к построению математических моделей стеганографических объектов*. Предлагаемый теоретико-информационный метод построения моделей стеганографических объектов основан на:

- особом подходе к стеганографической стойкости, заключающемся в исследовании стойкости стегосистемы к наилучшей возможной атаке, использующей заданный вектор характеристик;
- особом подходе к структуре стеганографического объекта, заключающемся в представлении объекта в качестве набора непересекающихся групп коэффициентов.

Пусть **c** – стеганографический контейнер. Зафиксируем некоторый вектор **f**(**c**) элементов стеганографического объекта **c**, распределение которых исследуется некоторым множеством стегоаналитических атак. В качестве критерия стойкости стегосистемы к стегоаналитическим атакам из этого множества можно рассматривать относительную энтропию $D\left(P_{\mathbf{f}} \,||\, \overline{P}_{\mathbf{f}}\right)$, где $P_{\mathbf{f}}$ – распределение вектора **f** элементов контейнера, а $\overline{P}_{\mathbf{f}}$ – распределение вектора **f** элементов стего. Вектор значений, которым описывается распределение вектора **f**(**c**), будем называть вектором характеристик стеганографического объекта.

Ключевой идеей предлагаемого подхода к структуре стеганографического объекта, контейнера или стего, является его представление в виде непересекающихся статистически однородных групп элементов, модифицируемых в процессе встраивания информации. Таким образом, стеганографический объект *c*, контейнер или стего, представлен в виде набора групп коэффициентов:

$$\mathbf{c} = \left\{\mathbf{c}^{(u)}\right\}_{u=1}^{u=g},$$

где $g$ – количество групп. Каждая группа $\mathbf{c}^{(u)}$ представляет собой вектор коэффициентов:

$$\mathbf{c}^{(u)} = \left\{c_i^{(u)}\right\}_{i=1}^{i=n_u},$$

где $n_u$ – количество элементов в *u*-й группе.

Построение модели стеганографического объекта в рамках этого метода подразумевает:

- разбиение множества элементов стеганографического объекта на непересекающиеся статистически однородные группы;
- выбор вектора характеристик, подаваемого стегоаналитиком на вход стегоаналитическим атакам;
- оценку распределения элементов контейнера на основе эмпирических данных;

- вычисление распределения элементов стего;
- вычисление относительной энтропии между распределениями элементов контейнеров и стего.

Вычисленная на последнем этапе относительная энтропия между распределениями элементов контейнеров и стего характеризует стойкость стегосистемы к наилучшей возможной атаке, использующей данный вектор характеристик.

*Метод повышения стойкости стеганографических систем.* Предлагаемый метод повышения стойкости стеганографических систем заключается в построении математической модели стеганографического объекта и решении следующей задачи нахождения оптимальной стратегии встраивания – вектора **x**, каждая компонента которого равна количеству битов сообщения, встраиваемых в соответствующую группу элементов контейнера:

$$D\left(P_{\mathbf{f}} \,||\, \overline{P}_{\mathbf{f}}(\mathbf{x})\right) \to \min$$

$$\mathbf{x} = \left\{x_i\right\}_{i=1}^{i=g},\ \sum_{u=1}^{g} x_u = l,\ 0 \le x_u \le k_u, u = 1, 2, \ldots, g,$$

где $l$ – количество битов во встраиваемом сообщении, $k_u$ – количество элементов $u$-й группы, которое может быть модифицировано при встраивании информации, $x_u$ – количество битов, встраиваемых в элементы $u$-й группы.

*Модель цифрового изображения в формате JPEG.* Квантованные DCT-коэффициенты цифрового изображения в формате JPEG разбиваются на 64 группы, принадлежность конкретного коэффициента группе определяется параметрами его вычисления в процессе применения дискретного косинусного преобразования к блоку из 64 пикселей изображения (иначе говоря, индексами коэффициента в блоке). Таким образом, одна из 64 групп состоит из DC-коэффициентов, остальные 63 группы – из AC-коэффициентов.

В качестве стеганографического алгоритма был выбран алгоритм nsF5 как наиболее стойкий метод встраивания информации в изображения в формате JPEG, не использующий стороннюю информацию.

Через $T$ обозначим максимальное возможное абсолютное значение DCT-коэффициента. В работе рассмотрены следующие векторы характеристик.

1. Дискретное распределение DCT-коэффициентов каждой из $g$ групп. Относительная энтропия между распределениями элементов контейнеров и стего вычисляется следующим образом:

$$D\left(P_H \,||\, \overline{P}_H(\mathbf{x})\right) = \sum_{u=1}^{g} n_u \sum_{i=-T}^{T} h_i^{(u)} \log_2 \frac{h_i^{(u)}}{\overline{h}_i^{(u)}},$$

где $h_i^{(u)} = P\left(c^{(u)} = i\right)$, $\overline{h}_i^{(u)} = P\left(\overline{c}^{(u)} = i\right)$.

2. Матрицы переходных вероятностей простой марковской цепи, образованной последовательностью абсолютных значений принадлежащих соседним блокам DCT-коэффициентов одной группы для каждой из $g$ групп. Относительная энтропия между распределениями элементов контейнеров и стего вычисляется следующим образом:

$$D\left(P_V \,||\, \overline{P}_V(\mathbf{x})\right) = \sum_{u=1}^{g} n_u \sum_{i=0}^{T} \sum_{j=0}^{T} v_{ij}^{(u)} h_i^{(u)} \log_2 \frac{v_{ij}^{(u)}}{\overline{v}_{ij}^{(u)}},$$

где $v_{ij}^{(u)} = P\left(\left|c_s^{(u)}\right| = j \middle| \left|c_{s-1}^{(u)}\right| = i\right)$, $\overline{v}_{ij}^{(u)} = P\left(\left|\overline{c}_s^{(u)}\right| = j \middle| \left|\overline{c}_{s-1}^{(u)}\right| = i\right)$.

3. Матрицы переходных вероятностей простой марковской цепи, образованной последовательностью разностей абсолютных значений соседних DCT-коэффициентов блока вдоль одного из четырех направлений: горизонтального, вертикального, вдоль главной диагонали, вдоль побочной диагонали. Вероятность $P\left(c_i^{(u)} = \alpha, \left|c_i^{(u)}\right| - \left|c_i^{(u_\lambda)}\right| = \sigma, \left|c_i^{(u_\lambda)}\right| - \left|c_i^{(u_{\lambda\lambda})}\right| = \tau\right)$ обозначим через $\mu_\alpha^{(u,\lambda)}(\sigma,\tau)$, где $\lambda \in \{h, v, d, m\}$ – одно из четырех направлений. Взаимное расположение коэффициентов в блоке в зависимости от направления $\lambda$ представлено на (рис. 1).

| | | | | |
|---|---|---|---|---|
| $c_i^{(u_{dd})}$ | | $c_i^{(u_{vv})}$ | | $c_i^{(u_{mm})}$ |
| | $c_i^{(u_d)}$ | $c_i^{(u_v)}$ | $c_i^{(u_m)}$ | |
| $c_i^{(u_{hh})}$ | $c_i^{(u_h)}$ | $c_i^{(u)}$ | | |

Рисунок 1 – Взаимное расположение элементов групп $u$, $u_h$, $u_{hh}$, $u_v$, $u_{vv}$, $u_d$, $u_{dd}$, $u_m$, $u_{mm}$ в $i$-м блоке коэффициентов

Вычисление относительной энтропии между распределениями элементов контейнеров и стего при использовании в качестве вектора характеристик матриц переходных вероятностей, описывающих корреляцию между DCT-коэффициентами блока вдоль направления $\lambda$:

$$D\left(P_{M^{(\lambda)}} \,\|\, \overline{P}_{M^{(\lambda)}}(\mathbf{x})\right) = \sum_{u=1}^{g} n_u \sum_{s=-T}^{T} \sum_{t=-T}^{T} m_{st}^{(u,\lambda)} \psi_s^{(u,\lambda)} \log_2 \frac{m_{st}^{(u,\lambda)}}{\overline{m}_{st}^{(u,\lambda)}},$$

где $\psi_s^{(u,\lambda)} = \sum_{\tau=-T}^{T} \sum_{\alpha=-T}^{T} \mu_\alpha^{(u,\lambda)}(s,\tau)$, $m_{st}^{(u,\lambda)} = P\left(\left|c_i^{(u_\lambda)}\right| - \left|c_i^{(u_{\lambda\lambda})}\right| = s \,\middle|\, \left|c_i^{(u)}\right| - \left|c_i^{(u_\lambda)}\right| = t\right)$,

$\overline{m}_{st}^{(u,\lambda)} = P\left(\left|\overline{c}_i^{(u_\lambda)}\right| - \left|\overline{c}_i^{(u_{\lambda\lambda})}\right| = s \,\middle|\, \left|\overline{c}_i^{(u)}\right| - \left|\overline{c}_i^{(u_\lambda)}\right| = t\right)$, $\lambda \in \{h, v, d, m\}$ – одно из четырех направлений.

4. Объединенный вектор характеристик. Через $w^{(u)}\left(a, b, \mathbf{t}, \tilde{\mathbf{t}}\right)$ обозначим вероятность $P\left(c_i^{(u)} = a, c_{i-1}^{(u)} = b, \mathbf{s}_{\mathbf{c}}^{(u,i)} = \mathbf{t}, \tilde{\mathbf{s}}_{\mathbf{c}}^{(u,i)} = \tilde{\mathbf{t}}\right)$, а через $w_{b,\mathbf{t}}^{(u)}\left(a, \tilde{\mathbf{t}}\right)$ и $\overline{w}_{b,\mathbf{t}}^{(u)}\left(a, \tilde{\mathbf{t}}\right)$ – соответственно условные вероятности $P\left(c_i^{(u)} = a, \tilde{\mathbf{s}}_{\mathbf{c}}^{(u,i)} = \tilde{\mathbf{t}} \;\middle|\; c_{i-1}^{(u)} = b, \mathbf{s}_{\mathbf{c}}^{(u,i)} = \mathbf{t}\right)$ и $P\left(\overline{c}_i^{(u)} = a, \tilde{\mathbf{s}}_{\overline{\mathbf{c}}}^{(u,i)} = \tilde{\mathbf{t}} \;\middle|\; \overline{c}_{i-1}^{(u)} = b, \mathbf{s}_{\overline{\mathbf{c}}}^{(u,i)} = \mathbf{t}\right)$, где $\mathbf{t} = \{t_i\}_{i=1}^{i=4}$, $\tilde{\mathbf{t}} = \{\tilde{t}_i\}_{i=1}^{i=4}$,

$\mathbf{s}_{\mathbf{c}}^{(u,i)} = \left\{\left|c_i^{(u)}\right| - \left|c_i^{(u_\lambda)}\right|\right\}_{\lambda=h,v,d,m}$, $\tilde{\mathbf{s}}_{\mathbf{c}}^{(u,i)} = \left\{\left|c_i^{(u_\lambda)}\right| - \left|c_i^{(u_{\lambda\lambda})}\right|\right\}_{\lambda=h,v,d,m}$.

Относительная энтропия между распределениями элементов контейнеров и стего вычисляется следующим образом:

$$D\left(P_W \,\|\, \overline{P}_W(\mathbf{x})\right) = \sum_{u=1}^{g} n_u \sum_{a=-T}^{T} \sum_{b=-T}^{T} \sum_{\mathbf{t}\in\Theta} \sum_{\tilde{\mathbf{t}}\in\Theta} w^{(u)}\left(a, b, \mathbf{t}, \tilde{\mathbf{t}}\right) \log_2 \frac{w_{b,\mathbf{t}}^{(u)}\left(a, \tilde{\mathbf{t}}\right)}{\overline{w}_{b,\mathbf{t}}^{(u)}\left(a, \tilde{\mathbf{t}}\right)},$$

где $\Theta = \left\{\mathbf{t} = \{t_i\}_{i=1}^{i=4} \,\middle|\, -T \le t_i \le T, 1 \le i \le 4\right\}$.

В этой главе получены формулы для вычисления всех вышеперечисленных векторов характеристик.

В **третьей главе** рассматривается задача целочисленной минимизации сепарабельной функции, к которой сводится задача нахождения оптимальной стратегии встраивания информации при построении математических моделей стеганографических объектов некоторых типов в соответствии с предлагаемым подходом.

В рамках данной работы предлагается эффективный алгоритм решения следующей задачи:

$$\begin{aligned} & D(\mathbf{x}) \to \min \\ & \mathbf{x} = \{x_i\}_{i=1}^{i=g},\ 0 \le x_i \le n,\ x_i \in \mathbf{Z},\ i = 1, 2, \ldots, g,\ \sum_{i=1}^{g} x_i = l, \end{aligned} \tag{1}$$

где $D(\mathbf{x}) = \sum_{i=1}^{g} d_i(x_i)$ – сепарабельная функция, а функции $d_i$ удовлетворяют следующим условиям:

1. $\Delta d_i(x_i) \ge 0$,
2. $\forall i\ \exists z_i,\ 0 < z_i < n$:

   $\Delta d_i(x_i) - \Delta d_i(x_i - 1) \ge 0$ при $x_i \le z_i$,

   $\Delta d_i(x_i) - \Delta d_i(x_i - 1) < 0$ при $n > x_i > z_i$.
3. $\forall i, j$: если $\exists x:\ \Delta d_i(x) < \Delta d_j(x)$, то $d_i(x) \le d_j(x)$, $\Delta d_i(x) \le \Delta d_j(x)$ для любого $x$, $0 < x \le n$.

Прежде чем перейти к описанию самого алгоритма, введем некоторые обозначения. Пронумеруем функции $d_i$ таким образом, что если $i > j$, то не существует такого $x$, что $\Delta d_i(x) < \Delta d_j(x)$.

Рассмотрим задачу минимизации:

$$\begin{aligned} & \sum_{i=u}^{g} d_i\left(y_i^{(u,l)}\right) \to \min \\ & y_i^{(u,l)} = 0,\ i = 1, 2, \ldots, u-1, \\ & \sum_{i=u}^{g} y_i^{(u,l)} = l,\ 0 \le y_i^{(u,l)} \le z_i,\ y_i^{(u,l)} \in \mathbf{Z},\ i = u, u+1, \ldots, g. \end{aligned} \tag{2}$$

Через $\mathbf{y}^{(u,l)} = \{y_i^{(u,l)}\}_{i=1}^{i=g}$ обозначим вектор, являющийся решением задачи (2), которое может быть получено с помощью эффективного «жадного» алгоритма.

Введем функции $f_u(l) = \sum_{i=u}^{g} d_i\left(y_i^{(u,l)}\right)$, $\Delta f_u(l) = f_u(l) - f_u(l-1)$ и $D_{u,l}(x_u) = \sum_{i=1}^{u-1} d_i(n) + d_u(x_u) + f_{u+1}(l - x_u - n(u-1))$, положим

$$\Delta D_{u,l}(x_u) = D_{u,l}(x_u) - D_{u,l}(x_u - 1) = \Delta d_u(x_u) - \Delta f_{u+1}(l - x_u + 1 - n(u-1)).$$

Также введем вектор $\mathbf{q} = \{q_i\}_{i=1}^{i=g}$, $q_i = y_i^{(i,l-n(i-1))}$.

Алгоритм решения задачи (1) состоит в следующем:

Шаг 1. Полагаем $k := \left\lfloor \frac{l}{n} \right\rfloor$;

Шаг 2. Полагаем $u := k$;

Шаг 3. Вычисляем $D_u := \min_{q_u \le x_u \le n} D_{u,l}(x_u)$, $\alpha_u := \arg\min_{q_u \le x_u \le n} D_{u,l}(x_u)$;

Шаг 4. Если $u > 1$ и $q_u < z_u$, то полагаем $u := u - 1$ и переходим к Шагу 3;

Шаг 5. Выбираем $v$ такое, что $D_v = \min_{s \le u \le k} D_u$;

Шаг 6. Результат: вектор $\bar{\mathbf{x}} = \{\bar{x}_i\}_{i=1}^{i=g}$:

$$\bar{x}_i = \begin{cases} n, & i < v, \\ \alpha_v, & i = v, \\ y_i^{(v+1,\,l-n(v-1)-\alpha_v)}, & i > v. \end{cases} \qquad (3)$$

Также в третьей главе доказываются следующие теоремы:

**Теорема.** Вектор $\bar{\mathbf{x}} = \{\bar{x}_i\}_{i=1}^{i=g}$, определенный согласно (3), является решением задачи (1).

**Теорема**. Асимптотическая сложность алгоритма равна $O(gl)$.

**Четвертая глава** посвящена описанию разработанного комплекса программ, реализующего предложенные модели, методы и алгоритмы, позволяющего исследовать влияние различных факторов на стойкость стеганографической системы, и проведенному вычислительному эксперименту.

С помощью проведенных экспериментов было исследовано влияние следующих факторов на стойкость встраивания информации в изображение в формате JPEG к наилучшей возможной атаке, использующей заданный вектор характеристик:

- размер скрываемого сообщения;
- стратегия встраивания информации, описывающей количество информации, встраиваемой в элементы каждой из групп;
- фактор качества изображений в формате JPEG;
- выбранный вектор характеристик;
- пороговые значения для различных векторов характеристик.

Также было исследовано влияние выбранной стратегии встраивания на стойкость стегосистемы к практическим стегоаналитическим атакам, использующим классификатор на основе метода опорных векторов.

В **заключении** перечислены основные результаты работы:

1. Исследованы существующие подходы к математическому моделированию стеганографических объектов, способы оценки и повышения стойкости стегосистем;
2. Предложен теоретико-информационный подход к построению математических моделей стеганографических объектов;
3. Построена математическая модель цифрового изображения в формате JPEG, позволяющая исследовать влияние количества встраиваемой информации и параметров скрывающего преобразования на стойкость системы;
4. Предложен метод повышения стойкости стеганографических систем;
5. Разработан эффективный вычислительный алгоритм решения возникающей при вычислении оптимальной стратегии встраивания для некоторых типов стеганографических объектов задачи минимизации сепарабельной функции;
6. Разработан комплекс программ, реализующий разработанные модели, методы и алгоритмы, позволяющий исследовать влияние различных

факторов на стойкость стеганографических систем с помощью вычислительных экспериментов;

7. Исследовано влияние различных факторов на стойкость стеганографической системы путем проведения вычислительного эксперимента.

**Список опубликованных работ по теме диссертации**

Публикации в изданиях из перечня рецензируемых научных журналов, рекомендуемых ВАК:


1. Разинков Е.В. Математическое моделирование стеганографических объектов / Е.В. Разинков // Ученые записки Казанского университета. Серия Физ.-мат. науки. – 2011. – Т. 153, кн. 4. – С. 176–188.
2. Разинков Е.В., Латыпов Р.Х. Стойкость стеганографических систем / Е.В. Разинков, Р.Х. Латыпов // Ученые записки Казанского государственного университета. Серия Физ.-мат. науки. – 2009. – Т. 151, кн. 2. – С. 126–132.
3. Разинков Е.В., Латыпов Р.Х. Скрытая передача информации с использованием границ объектов / Е.В. Разинков, Р.Х. Латыпов // Ученые записки Казанского государственного университета. Серия Физ.-мат. науки. – 2007. – Т. 149, кн. 2. – С. 128–137.


Прочие публикации:


4. Разинков Е.В., Латыпов Р.Х. О правиле выбора элементов стеганографического контейнера в скрывающем преобразовании / Е.В. Разинков, Р.Х. Латыпов // Прикладная дискретная математика (Приложение). – 2010. – №3. – С. 39–41.
5. Razinkov E.V., Latypov R.Kh. Image Steganograpghy Technique Using Objects Outlines / E.V. Razinkov, R.Kh. Latypov // Proc. of IEEE SMC UK&RI 6$^{th}$ Conference on Cybernetic Systems 2007, September 6–7, 2007. – P. 46–50.